Please find below and/or attached an Office communication concerning this application or proceeding.

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>04 August 2006</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>59-61,63-65,67,69-72 and 74-79</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) <u>71 and 79</u> is/are allowed.

6)☒ Claim(s) <u>59-61,63-65,67,69-72 and 74-79</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 08/04/06. The amendment filed

on 08/04/06 have been entered and made of record. Therefore, presently pending claims are 59-

61, 63-65, 67, 69-72, and 74-79.

Response to Arguments

Applicant's arguments filed 08/04/06 have been fully considered but they are not

persuasive because of following reasons.

In reference to the amendment wherein the port is closed to monitoring thereby

eliminating an open port, Daniel discloses sending data packets using email (column 3 lines 42-

49). Daniel further discloses creating, and therefore opening, input (inbound) and output

(outbound) ports (column 7 lines 51-60). Then after the TCPEmail process the ports are deleted

and therefore closed (column 8 lines 45-51). Therefore the remote network device is structured

to prevent any port from opening to monitor for an incoming request for reconfiguration from an

administrative site, thereby eliminating an open port for unauthorized access (fig. 8). The system

of Daniel discloses the port being closed (deleted) therefore removing the port from opening to

monitor for an incoming request for reconfiguration from any site and therefore an

administrative site. Further deleting the port eliminates the opening port for unauthorized access,

since it is deleted and therefore not available.

In reference to the amendment discloses retrieving the reconfiguration file without first

requiring a receipt of the incoming request, the system of Frailong retrieves the reconfiguration

file without first requiring receipt of an incoming request for reconfiguration from the

administration machine (column 17 lines 55-65). The retrieval is performed without a incoming

request because the reference discloses performing the retrieval automatically.

In response to applicant's argument that there is no suggestion to combine the references,

the examiner recognizes that obviousness can only be established by combining or modifying the

teachings of the prior art to produce the claimed invention where there is some teaching,

suggestion, or motivation to do so found either in the references themselves or in the knowledge

generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5

USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir.

1992). In this case, the motivation to combine was taken from the references.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

Claims 59 and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Frailong (6,230,194) in view of the book by Stallings (Network and Internetwork Security).

In reference to claim 59, Frailong suggests a secure system for configuring remote

networked devices and gateway servers, comprising: an administration machine structured to

create, update and maintain a configuration data file (column 5 lines 23-32 and column 12 lines

5-13), the administration machine comprising a storage device structured to temporarily store the

configuration data file (column 10 lines 1-3), the administration machine further structured to

retrieve the configuration data file from the storage device (column 5 lines 15-23), the

administration machine further comprising a network interface structured to interface with a

network (column 12 lines 5-9) the administrative machine further structured to transmit the

encrypted file to a remote email server (column 7 lines 60-63 and column 14 line 63 to column

15 line 15); a remote email server structured to receive the encrypted file from the administration

machine and to temporarily store the encrypted file (column 15 lines 16-21); a remote gateway

server comprising a remote network interface structure to interface with the network (column 6

lines 19-26), the remote network interface comprising at least one remote inbound

communication port and at least one remote outbound communication port (column 6 lines 26-

29), the remote network interface is further structured to retrieve the encrypted file from the

remote email server (column 15 lines 64-67), the remote gateway server further comprising a

remote storage device to store the encrypted file (column 5 line 58 to column 6 line 18), the

remote gateway server structured to access the encrypted file from the remote storage device and

decrypt the encrypted file to generate a decrypted configuration data file (column 5 lines 41-56),

the remote gateway server further structured to reconfigure at least one configuration parameter

of the remote gateway server in accordance with the decrypted configuration data file (column 8

lines 35-62). The system of Frailong retrieves the reconfiguration file without first requiring

receipt of an incoming request for reconfiguration from the administration machine (column 17

lines 55-65). The retrieval is performed without a incoming request because the reference

discloses performing the retrieval automatically.

However Frailong does not disclose compressing the file before sending it.

Stallings discloses compressing the message to save space for e-mail transmission (page

366) and further encryption applied after compression.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to compress the data for e-mail transmission as disclosed by Stalling in the system

of Frailong. One of ordinary skill in the art would have been motivated to do this because

compression would save space for email transmission (page 366).

Although Frailong suggests the use of email to send messages (configuration data) to the

gateway server, Frailong does not disclose an inbound (input) and output (outbound) ports.

However, as disclosed above, the applicant claims ports that have contradictory functions.

Therefore, to continue prosecution, the examiner assumes that the applicant meant that the

administration machine and the gateway server have a communication interface for receiving and

sending messages using ports. The device opens the ports in order to receive email, including

the configuration. Then closes the port after the messages have been received or sent.

In reference to claim 63 wherein the remote gateway server is further structured to

periodically poll the remote server to identify an encrypted file to be retrieved from the remote

email server by the remote gateway server (Part 1016 Fig. 10).

Claims 60-61, 64-65, 67, 69-71 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Frailong (6,230,194) in view of the book by Stallings (Network and

Internetwork Security) and further in view of Daniel (6,272,549).

In reference to claim 64, Frailong suggests a secure system for configuring remote

networked devices and gateway servers, comprising: an administration machine structured to

create, update and maintain a configuration data file (column 5 lines 23-32 and column 12 lines

5-13), the administration machine comprising a storage device structured to temporarily store the

configuration data file (column 10 lines 1-3), the administration machine further structured to

retrieve the configuration data file from the storage device (column 5 lines 15-23), the

administration machine further comprising a network interface structured to interface with a

network (column 12 lines 5-9) the administrative machine further structured to transmit the

encrypted file to a remote email server (column 7 lines 60-63 and column 14 line 63 to column

15 line 15); a remote email server structured to receive the encrypted file from the administration

machine and to temporarily store the encrypted file (column 15 lines 16-21); a remote gateway

server comprising a remote network interface structure to interface with the network (column 6

lines 19-26), the remote network interface comprising at least one remote inbound

communication port and at least one remote outbound communication port (column 6 lines 26-

29), the remote network interface is further structured to retrieve the encrypted file from the

remote email server (column 15 lines 64-67), the remote gateway server further comprising a

remote storage device to store the encrypted file (column 5 line 58 to column 6 line 18), the

remote gateway server structured to access the encrypted file from the remote storage device and

decrypt the encrypted file to generate a decrypted configuration data file (column 5 lines 41-56),

the remote gateway server further structured to reconfigure at least one configuration parameter

of the remote gateway server in accordance with the decrypted configuration data file (column 8

lines 35-62). Frailong discloses a remote network device structured to retrieve the at least one

file from the remote staging platform in response to a polling of the remote staging platform by

the at least one remote network device (column 15 lines 64-67 and Fig. 10).

However Frailong does not disclose compressing the file before sending it.

Stallings discloses compressing the message to save space for e-mail transmission (page 366) and further encryption applied after compression.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to compress the data for e-mail transmission as disclosed by Stalling in the system of Frailong. One of ordinary skill in the art would have been motivated to do this because compression would save space for email transmission (page 366).

Although Frailong suggests the use of email to send messages (configuration data) to the gateway server, Frailong does not disclose an inbound (input) and output (outbound) ports. However, as disclosed above, the applicant claims ports that have contradictory functions. Therefore, to continue prosecution, the examiner assumes that the applicant meant that the administration machine and the gateway server have a communication interface for receiving and sending messages using ports. The device opens the ports in order to receive email, including the configuration. Then closes the port after the messages have been received or sent.

Frailong does not expressly disclose opening and closing the ports to receive the email, configuration data, and when the email is received.

Daniel discloses sending data packets using email (column 3 lines 42-49). Daniel further discloses creating, and therefore opening, input (inbound) and output (outbound) ports (column 7 lines 51-60). Then after the TCPEmail process the ports are deleted and therefore closed (column 8 lines 45-51). Therefore the remote network device is structured to prevent any port from opening to monitor for an incoming request for reconfiguration from an administrative site, thereby eliminating an open port for unauthorized access (fig. 8). The system of Daniel discloses

the port being closed (deleted) therefore removing the port from opening to monitor for an

incoming request for reconfiguration from any site and therefore an administrative site. Further

deleting the port eliminates the opening port for unauthorized access, since it is deleted and

therefore not available.

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to open the ports when receiving email and then closing them when the process is

complete as in the system of Daniel in the system of Frailong. One of ordinary skill in the art

would have been motivated to do this because closing the ports would free the memory (Daniel

column 8 lines 51-52).

In reference to claims 60 and 65, wherein the network interface is further structured to

transmit the encrypted file to the remote email server through the at least one outbound

communication port of the administrative machine via standard mail transfer protocol.

Daniel discloses using SMTP to transmit the data between computer systems (column 8

lines 32-38).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to open the ports when receiving email and then closing them when the process is

complete as in the system of Daniel in the system of Frailong. One of ordinary skill in the art

would have been motivated to do this because closing the ports would free the memory (Daniel

column 8 lines 51-52).

In reference to claims 61 and 67, wherein the remote network interface is further

structured to retrieve the encrypted file from the remote email server through the at least one

remote outbound communication port of the remote gateway server via standard mail transfer

protocol.

Frailong discloses the transmission of the encrypted file from the ISP (which provides email services) to through the at least one remote outbound communication port of the remote gateway server (column 6 lines 19-32).

Daniel discloses using SMTP to transmit the data between computer systems (column 8 lines 32-38).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to open the ports when receiving email and then closing them when the process is complete as in the system of Daniel in the system of Frailong. One of ordinary skill in the art would have been motivated to do this because closing the ports would free the memory (Daniel column 8 lines 51-52).

In reference to claim 70, wherein the remote gateway server is further structured to periodically poll the remote server to identify an encrypted file to be retrieved from the remote email server by the remote gateway server (Part 1016 Fig. 10).

In reference to claim 69, wherein no direct communication pathway is established between the administrative site and the remote network device to transmit or retrieve the at least one file via standard mail transfer protocol (column 4 lines 58-67).

In reference to claim 62 wherein the network interface is further structured such that no inbound communication port is open at the administrative machine to transmit the encrypted file to the remote email server. Due to the contradictions discussed in the 35 U.S.C. 112 rejection above, claims 62 and 68 are rejected as the claim 60. Therefore the examiner assumes that there is a port that is open to send the information to the remote email server.

Claims 72, 74, and 75 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Frailong in view of Stallings as rejected in claim 59 and further in view of Smith (6,532,543).

In reference to claim 72, Frailong, Stalling, disclose the claimed subject matter as

discussed in claim 59.

However neither Frailong, Stallings, and Daniel discuss creating a configuration database

with encrypted data from the configuration database to produce and encrypted file.

Smith discloses a method for securely configuring remote networked devices, comprising

the steps of: creating a configuration database (column 17 lines 34-38); encrypting data from the

configuration database to produce an encrypted file (column 22 lines 24-28); transmitting the

encrypted file to a remote device (column 22 lines 24-26).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to create a database as in the system of Smith in the system of Frailong. One of

ordinary skill in the art would have been motivated to do this because databases are methods of

organizing data in a convenient and easy way.

In reference to claim 74, wherein no direct communication pathway is established

between the administrative site and the remote network device to transmit or retrieve the at least

one file via standard mail transfer protocol (column 4 lines 58-67).

In reference to claim 75, further comprising the step of creating a confirmation message

upon successful reconfiguration of the remote gateway server (Fig. 12).

Claims 76-78 are rejected under 35 U.S.C. 103(a) as being unpatentable over Frailong in

view of Stallings and further in view of Smith as rejected in claim 72 and further in view of

Smith (6,532,543).

In reference to claim 76, further comprising the step of transmitting the confirmation

message from the remote gateway device to the remote email server through the at least one

remote outbound communication port of the remote gateway device via standard mail transfer

protocol

Frailong discloses transmitting the confirmation message (Fig. 12).

Frailong does not expressly disclose the use of SMTP.

Daniel discloses using SMTP to transmit the data between computer systems (column 8

lines 32-38).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to open the ports when receiving email and then closing them when the process is

complete as in the system of Daniel in the system of Frailong. One of ordinary skill in the art

would have been motivated to do this because closing the ports would free the memory (Daniel

column 8 lines 51-52).

In reference to claim 77, further comprising the step of retrieving the confirmation

message from the remote email server by the administrative site through the at least one

outbound communication port of the administrative site via standard mail transfer protocol.

Frailong discloses retrieving the confirmation message (Fig. 12).

Frailong does not expressly disclose the use of SMTP.

Daniel discloses using SMTP to transmit the data between computer systems (column 8

lines 32-38).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to open the ports when receiving email and then closing them when the process is complete as in the system of Daniel in the system of Frailong. One of ordinary skill in the art would have been motivated to do this because closing the ports would free the memory (Daniel column 8 lines 51-52).

In reference to claim 78, further comprising the steps of generating a configuration failure message at the administrative site when no confirmation message is retrieved from the remote email server within a predetermined time period after transmittal of the encrypted file and transmitting the configuration failure message from the administrative site through the at least one outbound communication port to a remote gateway device manager via standard mail transfer protocol.

Frailong discloses generating a confirmation failure message at the gateway site which is sent to remote server (Fig. 12).

Frailong does not expressly disclose the use of SMTP.

Daniel discloses using SMTP to transmit the data between computer systems (column 8 lines 32-38).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to open the ports when receiving email and then closing them when the process is complete as in the system of Daniel in the system of Frailong. One of ordinary skill in the art would have been motivated to do this because closing the ports would free the memory (Daniel column 8 lines 51-52).

Allowable Subject Matter

Claims 71 and 79 allowed.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854.

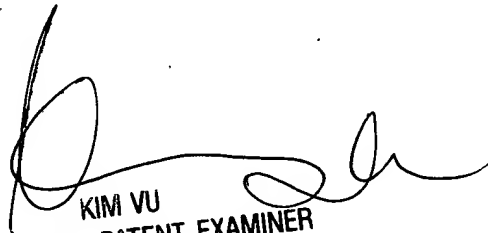The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, October 16, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100